

**REMARKS**

The specification has been amended to correct errors of a typographical and grammatical nature. Due to the number of corrections thereto, applicants submit herewith a Substitute Specification, along with a marked-up copy of the original specification for the Examiner's convenience. The substitute specification includes the changes as shown in the marked-up copy and includes no new matter. Therefore, entry of the Substitute Specification is respectfully requested.

The abstract has also been amended to more clearly describe the features of the present invention.

Entry of the preliminary amendments and examination of the application is respectfully requested.

To the extent necessary, applicant's petition for an extension of time under 37 CFR 1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (Case: 501.42780X00) and please credit any excess fees to such deposit account.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



---

Carl I. Brundidge  
Registration No. 29,621

DRAAES/jla  
(703) 312-6600

VERSION WITH MARKINGS TO SHOW CHANGES

IN THE ABSTRACT:

An object of the present invention is to provide a smart card and a settlement terminal are provided by which, when common-key cryptography is used for value transfer between smart cards, the security of the whole system can be improved by enabling easy updating of a cryptographic key used for the value transfer.

A smart card transmits/receives value data to/from another smart card. The smart card includes an information accumulating means-unit for accumulating the value data, a transfer key used to update the value data, and an update key used to update the transfer key; a communication means-unit for receiving a transfer key encrypted by use of the update key, the transfer key being transmitted from another smart card; and an arithmetic processing means-unit for decrypting the encrypted transfer key by use of the update key to update the transfer key accumulated in the information accumulating means-unit by use of the decrypted transfer key.